Salisbury University

Asset Management Policy

1. PURPOSE

Compiling and maintaining inventory and accountability of assets is an important aspect of risk management. According to the *Security Assessment Policy*, each asset or class of asset must be assigned a security category based on its perceived level of confidentiality, integrity, and availability, and it is the role of **asset management** to inventory, account for, and track these assets.

2. REVISION HISTORY

Date	Version	Approved By:	Policy Update
12/18/2017	1.0	Dr. Dudley-Eshbach	Initial Publication

3. SCOPE

This policy is applicable to all Salisbury University Information Technology (SUIT) department managed assets owned by Salisbury University.

4. BASE POLICY AND COMPLIANCE REFERENCES

SUIT policy framework is based upon federal, state, and industry best practices and standards. Below is a listing of the base policy and compliance references from University System of Maryland (USM), Federal, State, and other organizations. This policy serves as SU's authoritative adaptation of these policies with specific amendments to meet the business and operational needs of the University.

Policy References

- State of Maryland Department of IT - Cybersecurity Policy: http://doit.maryland.gov/Pages/DoIT-Policy-List.aspx
- USM Security Guidelines: http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

5. POLICY

This policy describes an overall strategy to implement asset management processes within the SUIT infrastructure.

5.1 General Requirements

SUIT is responsible to maintain an accurate and timely inventory of trackable SUIT managed assets within Salisbury University (SU). SUIT will observe the requirements shown in section 5.1.1 below:

5.1.1 Minimum Requirements for Asset Management

#	Name	Requirement
A	Asset Inventory and Tracking	Track and account for SUIT owned & managed assets, including: physical devices, software licenses, and data IT assets where possible (as defined in section 7.0).
B	Periodic Audit	Conduct a regular audit of physical tagged SUIT assets and reconcile the audit with the SUIT asset inventory. Investigate and resolve discrepancies between the physical audit of IT assets and the IT asset inventory.
C	Periodic Updates	Where possible update and maintain the asset inventory as assets are acquired, configured, deployed, or disposed of throughout the asset lifecycle. Note the relevant information is dependent on the asset type.
D	Automated Asset Inventory	Implement an automated mechanism to support tracking of information system assets, where possible.

5.2 Types of Assets

5.2.1 Physical IT Assets

Physical SUIT assets, where possible, will be tracked and accounted for. SUIT owned & managed physical devices should maintain as much of the following information as applicable in relevant management systems for each type of device.

#	Name	Requirement
A	Physical Assets	Maintain an inventory of physical SUIT owned & managed assets.
B	Contacts	Where possible, determine through automated tools the primary user of a device for single-user assets, or for shared-use assets identify the owning department.
C	Type	Identify the physical device type that will have an SU inventory tag such as: ▪ Desktop ▪ Storage Appliance ▪ Laptop ▪ Network Appliance ▪ Tablet Server
D	Hardware Identification	Identify and record the relevant information to identify the hardware such as a device manufacturer, make, model or serial number.
E	Physical Location	If the device is primarily stationary, identify the location and where possible include building address and room number
F	Logical Identification	▪ Record relevant logical identifiers for the device such as a device name or network address information if applicable.
		▪ IP address(es) (if static) ▪ Host name ▪ Domain membership ▪ MAC address(es)
G	Operating System	Record the type and version of the operating system installed on the device where possible.

H	Security Categorization	Record the security categorization of the device if the risk deviates from the general classification of the type of device it belongs to wherever possible.
I	Purpose	Record the general purpose of the device where applicable.
J	Asset Tag	Each physical asset should be affixed with an asset tag, which will include a unique asset identifier.
K	Date	Record the date on which the item was entered into and/or removed from inventory where possible.

5.2.2 Software Assets

SUIT should maintain a Software Management Database to document SUIT owned and managed software licenses. This database will store relevant information for managed software and where possible contain the following information about each piece of managed software:

#	Name	Requirement
A	Software Assets	Maintain a database of SUIT owned and managed software licenses supported for use within Salisbury University.
B	Supported Software	Agencies shall maintain a database of supported applications. This database should include the following information where possible and relevant: ▪ Software Vendor ▪ Software Title ▪ Version Exception: Specialized appliances for which the agency has no control at the operating system level.
C	Installed Software by Device	Use an automated tool where possible to identify the software installed on end user workstations.
D	Licensing	If the managed software is restricted by a licensing agreement, maintain the details of that license agreement and if required to do so by the licensor, track the usage of that license through applicable tools where possible.

5.2.3 Data Assets

The SUIT department is responsible for identifying and protecting assets that contain or are responsible for transmission of confidential data where possible. Significant repositories of SUIT managed confidential data should be protected per the following guidelines below.

#	Name	Requirement
A	Data Assets	Identify and maintain an accurate list of SUIT managed repositories of confidential data.
B	Confidential Data Types	Confidential data is defined by the *SU Public and Confidential Data Policy*.

C	Confidential Data: Major Repositories	Identify all major repositories of confidential data where possible. Depending on the nature of the data repository, relevant identifying information about the repository should be recorded as well as the scope of data risk.
D	Confidential Data: Major Transit Routes	Identify all major network transit routes, to and from major confidential data repositories, documented in the form of a topology diagram.
E	Confidential Data Detection	Where possible, confidential data should be automatically detected on managed systems.

5.2.4 Copyright Violations

Any violation of electronic asset copyright or licensing agreements is to be reported to and tracked by copyright@salisbury.edu.

6. EXEMPTIONS

If an exemption from this policy is required, an SUIT Policy Exemption Form needs to be submitted and it needs to clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks associated with this exemption. If the University can accept the risk, an exemption to this policy may be granted.

7. DEFINITIONS

Term	Definition
Asset Management	The method for identifying, procuring, maintaining, tracking, and disposing of all information technology assets.
Information Technology (SUIT) Assets	SUIT Assets include SU owned and managed physical devices, supported software, and major confidential data repositories
Software Management Database	A central repository for managing and inventorying SUIT owned & supported Software license information.

8. ENFORCEMENT

SUIT is responsible for managing security assessments for the University according to established requirements authorized in the SUIT Security Program Policy. Any systems under the policy authority of SUIT with requirements that deviate from the SUIT Security Program policies are required to submit a Policy Exemption Form to SUIT for consideration and potential approval.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.